

Comment on “Security analysis and improvements of arbitrated quantum signature schemes”

Tzonelih Hwang*, Yi-Ping Luo, Song-Kong Chong

February 13, 2012

Abstract

Recently, Zou et al. [Phys. Rev. A 82, 042325 (2010)] demonstrated that two arbitrated quantum signature (AQS) schemes are not secure, because an arbitrator cannot arbitrate the dispute between two users when a receiver repudiates the integrity of a signature. By using a public board, Zou et al. proposed two AQS schemes to solve the problem. This work shows that the same security problem may exist in Zou et al.’s schemes. Moreover, a malicious verifier, Bob, can actively negate a signed order if he wants to. This attack, a special case of denial-of-service (DoS) attack mentioned in [Phys. Rev. Lett. 91, 109801 (2003)], is important in quantum cryptography. Bob may get some benefits with this DoS attack, since he can actively deny Alice’s signed order without being detected. This work also shows that a malicious signer can reveal the verifier’s secret key without being detected by using Trojan-horse attacks.

Keywords: Quantum information; Quantum cryptography; Arbitrated quantum signature.

*Corresponding Author

1 Introduction

The quantum signature, which provides the authenticity and non-repudiation of quantum states on an insecure quantum channel [1, 2], is one of the most important topics of research in quantum cryptography. The quantum signature can provide unconditional security by exploiting the principles of quantum mechanics, such as the no-cloning theory and measurement uncertainty. Two basic properties are required in a quantum signature [1] :

1. Unforgeability: Neither the signature verifier nor an attacker can forge a signature or change the content of a signature. The signature should not be reproducible by any other person.
2. Undeniability: A signatory, Alice, who has sent the signature to the verifier, Bob, cannot later deny having provided a signature. Moreover, the verifier Bob cannot deny the receipt of a signature.

The first quantum signature was proposed by Gottesman and Chuang [3]. Subsequently, a variety of quantum signature schemes have been proposed [1, 2, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14]. Zeng et al. [1] proposed an arbitrated quantum signature (AQS) scheme based on the correlation between Green-Horne-Zeilinger (GHZ) states and quantum one-time pads. However, Curty et al. [6] pointed out that this AQS scheme [1] is not clearly described and that the security statements claimed by the authors are incorrect. In response [7], Zeng provided a more detailed presentation and proof to Zeng et al.'s original AQS scheme [1]. To improve the transmission efficiency and to reduce the implementation complexity of [1, 7], Li et al. [8] proposed an AQS scheme using Bell states and claimed that their improvements can preserve the merits in the original scheme [1, 7].

In an AQS scheme, the arbitrator plays a crucial role. When a dispute arises between users, the arbitrator should be able to arbitrate the dispute. In other words, the arbitrator should be able to solve a dispute when a verifier, Bob, repudiates the receipt of a signature or, in particular, when the verifier repudiates the integrity of a signature, i.e., Bob admits receiving a signature but denies the correctness of the signature. The latter dispute implies one of the following three cases [15]:

- (1) Bob told a lie;
- (2) The signatory Alice sent incorrect information to Bob;
- (3) An eavesdropper Eve disturbed the communications.

As the arbitrator in [1, 7, 8] cannot solve the dispute when Bob claims that the verification of a signature is not successful, Zou et al. [15] considered that these schemes are not valid AQS schemes because the security requirement of a quantum signature, i.e., undeniability, is not satisfied.

By using a public board, Zou et al. also proposed two AQS schemes to solve the problem. However, this study demonstrates that the same security problem may exist in Zou et al.'s schemes. In their schemes, when Bob announces that the verification of a signature is not successful, the arbitrator may not be able to arbitrate the dispute mentioned above. Moreover, a malicious verifier, Bob, can actively negate a signature if he wants to. This attack, a special case of denial-of-service (DoS) attack mentioned in [16], is important in quantum cryptography. Bob may get some benefits with this DoS attack, since he can actively deny Alice's signature without being detected. In addition, this study attempts to demonstrate that a malicious signer, Alice, can reveal Bob's secret key without being detected by using Trojan-horse attacks [17, 18].

The rest of this paper is organized as follows. Section 2 reviews one of Zou et al.'s schemes. Section 3 discusses the problems with the scheme. Finally, Section 4 summarizes the result.

2 Review of Zou et al.'s first signature scheme

Zou et al.'s first AQS scheme [15] is briefly explained in the following scenario. Alice, the message signatory, wants to sign a quantum message $|P\rangle$ to a signature verifier, Bob, via the assistance of an arbitrator, Trent. Suppose that Alice and Bob share a secret key $K \in \{0, 1\}^*$ and that the quantum message to be signed is $|P\rangle = |P_1\rangle \otimes |P_2\rangle \otimes \dots \otimes |P_n\rangle$, where $|K| \geq 2n$, $|P_i\rangle = \alpha_i |0\rangle + \beta_i |1\rangle$, and $1 \leq i \leq n$. In order to protect the quantum message, the quantum one-time-pad encryption E_K [19] and the unitary transformation M_K used in the schemes are defined as follows.

$$E_K(|P\rangle) = \bigotimes_{i=1}^n \sigma_x^{K_{2i-1}} \sigma_z^{K_{2i}} |P_i\rangle, \quad (1)$$

$$M_K(|P\rangle) = \bigotimes_{i=1}^n \sigma_x^{K_i} \sigma_z^{K_{i\oplus 1}} |P_i\rangle, \quad (2)$$

where $|P_i\rangle$ and K_i denote the i th bit of $|P\rangle$ and K , respectively, and σ_x and σ_z are the respective Pauli matrices.

To prevent the integrity of a signature from being repudiated by Bob, Zou et al. proposed two AQS schemes: the AQS scheme using Bell states and the AQS without using entangled states. In this paper, we only review their AQS scheme using Bell states.

Suppose that Alice wants to sign an n -qubit quantum message $|P\rangle$ to Bob. In order to perform the signature, three copies of $|P\rangle$ are necessary. The scheme proceeds as follows:

Initialization phase:

Step I1. The arbitrator Trent shares the secret keys K_A and K_B with Alice and Bob, respectively, through some unconditionally secure quantum key distribution protocols.

Step I2. Alice generates n Bell states, $|\psi_i\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$, where $1 \leq i \leq n$; the subscripts A and B denote the first and second particles of the Bell state, respectively. After that, Alice sends all B particles to Bob in a secure and authenticated way [20, 21].

Signing phase:

Step S1. Alice chooses a random number $r \in \{00, 01, 10, 11\}^n$ to encrypt all $|P\rangle$'s, i.e., $|P'\rangle = E_r(|P\rangle)$.

Step S2. Alice generates $|S_A\rangle = E_{K_A}(|P'\rangle)$.

Step S3. Alice combines each $|P'_i\rangle$ with the first particle A of each Bell state. Then, each original Bell state becomes a three-particle entangled state,

$$|\phi_i\rangle_{PAB} = |P'_i\rangle \otimes |\psi_i\rangle_{AB} = \frac{1}{2} \left[\begin{array}{l} |\Phi_{PA}^+\rangle_i (\alpha'_i |0\rangle + \beta'_i |1\rangle)_B + |\Phi_{PA}^-\rangle_i (\alpha'_i |0\rangle - \beta'_i |1\rangle)_B + \\ |\Psi_{PA}^+\rangle_i (\alpha'_i |1\rangle + \beta'_i |0\rangle)_B + |\Psi_{PA}^-\rangle_i (\alpha'_i |1\rangle - \beta'_i |0\rangle)_B \end{array} \right],$$

where $|\Phi_{PA}^+\rangle, |\Phi_{PA}^-\rangle, |\Psi_{PA}^+\rangle$, and $|\Psi_{PA}^-\rangle$ are the four Bell states [22].

Step S4. Alice performs a Bell measurement on each pair $|\phi_i\rangle_{PA}$ and obtains the measurement results $|M_A\rangle = (|M_A^1\rangle, |M_A^2\rangle, \dots, |M_A^n\rangle)$, where $|M_A^i\rangle \in \{|\Phi_{PA}^+\rangle_i, |\Phi_{PA}^-\rangle_i, |\Psi_{PA}^+\rangle_i, |\Psi_{PA}^-\rangle_i\}$, and $1 \leq i \leq n$.

Step S5. Alice sends $|S\rangle = (|P'\rangle, |S_A\rangle, |M_A\rangle)$ to Bob.

Verification phase:

Step V1. Bob encrypts $|P'\rangle$ and $|S_A\rangle$ with K_B and sends the quantum ciphertext $|Y_B\rangle = E_{K_B}(|P'\rangle, |S_A\rangle)$ to Trent.

Step V2. Trent decrypts $|Y_B\rangle$ with K_B and obtains $|P'\rangle$ and $|S_A\rangle$. Next, he encrypts $|P'\rangle$ with K_A and obtains $|S_T\rangle$. If $|S_T\rangle = |S_A\rangle$ [8, 23], then Trent sets the verification parameter $V = 1$; otherwise, he sets $V = 0$.

Step V3. Trent recovers $|P'\rangle$ from $|S_T\rangle$. Then, he encrypts $|P'\rangle, |S_A\rangle$, and V with K_B and sends the quantum ciphertext $|Y_T\rangle = E_{K_B}(|P'\rangle, |S_A\rangle, V)$ to Bob.

Step V4. Bob decrypts $|Y_T\rangle$ and obtains $|P'\rangle, |S_A\rangle$, and V . If $V = 0$, Bob rejects the signature; otherwise, Bob continues to the next step.

Step V5. Based on Alice's measurement results M_A , Bob can obtain $|P'_B\rangle$ from the B particles received from the Step **I2**, according to the principle of teleportation [8]. Next, he compares $|P'_B\rangle$ with $|P'\rangle$. If $|P'_B\rangle = |P'\rangle$, Bob informs Alice to publish r and proceeds to the next step; otherwise, he rejects the signature.

Step V6. Alice publishes r on the public board.

Step V7. Bob recovers $|P\rangle$ from $|P'\rangle$ by r and holds $(|S_A\rangle, r)$ as Alice's signature for the quantum message $|P\rangle$.

3 Discussion on Zou et al.'s scheme

This section discusses problems that could arise in Zou et al.'s scheme if precautions are not taken. We first present a DoS attack by using undeniability dilemma and give an example to show that a verifier can actively negate a signature without being detected to get some benefits in his favor. Then, we introduce Trojan-horse attacks to Zou et al.'s scheme.

3.1 Undeniability dilemma - A Denial-of-service (DoS) attack

In Zou et al.'s scheme, the signatory Alice uses a random number r to protect the quantum message $|P\rangle$ (i.e., $|P'\rangle = E_r(|P\rangle)$) before signing it. After the verification by the arbitrator Trent, Bob recovers $|P'_B\rangle$ and compares it with $|P'\rangle$. Once Bob informs Alice that $|P'_B\rangle = |P'\rangle$, Alice publishes r on the public board, which is assumed to be free from being blocked, injected, or altered. Finally, Bob recovers $|P\rangle$ from $|P'\rangle$ by r and retains $(|S_A\rangle, r)$ as Alice's signature.

It appears that if Bob informs Alice to publish r on the public board, then he cannot disavow the integrity of the signature. In accordance with this logic, Zou et al. considered that the use of the public board can prevent the denial attack from Bob. However, if Bob claims that $|P'_B\rangle \neq |P'\rangle$ in Step V5 before requesting the value of r from Alice, then Trent cannot arbitrate the dispute between Alice and Bob because one of the following three possible cases may occur.

1. Bob told a lie: In this case, Bob decides to forego the recovery of the message $|P\rangle$ due to some reasons;
2. Alice sent incorrect information to Bob: In Step S3, Alice deliberately generated $|\phi_i\rangle$ using another message $|\hat{P}'_i\rangle$ with $|\hat{P}'_i\rangle \neq |P'_i\rangle$ or generated $|S\rangle = (|P'\rangle, |S_A\rangle, |M'_A\rangle)$ with $|M'_A\rangle \neq |M_A\rangle$ in Step S5;
3. Eve disturbed the communication.

Apparently, when Bob claims that $|P'_B\rangle \neq |P'\rangle$ in this case, Trent cannot solve the dispute. Hence, Bob can perform the DoS attack by negating the signature from Alice without being detected. Furthermore, as also pointed out in [15], Alice is able to publish an arbitrary value $r' (\neq r)$ such that the original signature cannot be verified successfully by Bob, which is also contradictory to the

undeniable requirement of a signature scheme.

This problem could be serious if the signature occurs in an electronic order system, where Alice is a buyer and Bob, a company. Bob is able to negate a signed order from Alice if the current market situation is not in his favor. In such a case, it does not matter whether Bob can obtain the value r to recover the signed order from Alice, because Bob knows that due to the order, he will lose a fortune. Similarly, by controlling the value of r , Alice is also able to select a situation favorable to her for completing the signature process.

The same dilemma may occur in Zou et al.'s second AQS scheme.

3.2 Trojan-horse attacks

In Zou et al.'s scheme, there are two transmissions of the same quantum signals, first from Alice to Bob and then from Bob to Trent. Therefore, the malicious Alice can reveal Bob's secret key without being detected by using Trojan-horse attacks [17, 18]. As pointed out in [5], there are two ways to use Trojan-horse attacks: invisible photon eavesdropping (IPE)[17] and delay photon eavesdropping [18]. Here, we discuss the IPE attack on Zou et al.'s scheme and demonstrate that Alice can obtain Bob's secret key without being detected. It should be noted that Alice can also use the delay photon eavesdropping to reveal Bob's secret key in the same way.

In order to reveal Bob's secret key K_B , Alice can use the IPE attack on the communications in Step $S5$ and Step $V1$ as follows:

Step $S5a$. Alice first prepares a set of eavesdropping states, $D^i \in \left\{ \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)_{d_1^i d_2^i} \right\}$, as invisible photons, where the subscripts d_1^i and d_2^i represent the first and second photons, respectively, in D^i , $1 \leq i \leq n$. For each state in $|P'\rangle$ (or $|S_A\rangle$), Alice inserts d_1^i as an invisible photon to that state and forms a new sequence $|P'\rangle^{d_1}$ ($|S_A\rangle^{d_1}$). Next, Alice sends $|S\rangle^{d_1} =$

$(|P'\rangle^{d_1}, |S_A\rangle, |M_A\rangle)$ to Bob.

Step V1a. Bob encrypts $|P'\rangle^{d_1}$ and $|S_A\rangle$ with K_B and sends the quantum ciphertext $|Y_B\rangle^{d_{1'}} = E_{K_B}(|P'\rangle^{d_1}, |S_A\rangle)$ to Trent. Before Trent receives the quantum ciphertext $|Y_B\rangle^{d_{1'}}$, Alice captures $d_{1'}$ from $|Y_B\rangle^{d_{1'}}$ and measures d_1, d_2 together with the Bell measurement. According to the measurement result of d_1^i, d_2^i , Alice can obtain Bob's secret key $K_B^{2i-1, 2i}$.

It should be noted that Alice can similarly use the process mentioned above to obtain Bob's secret key K_{BT} in Zou et al.'s second AQS scheme. Since both schemes are susceptible to Trojan-horse attacks, Bob can deny having verified a signature.

To prevent the scheme from Trojan-horse attacks, it is well-known that two additional devices, a wavelength filter and a photon number splitter (PNS) can be added to the protocol. By letting the received photons pass through both devices, the photons with different wavelength or the delay photons will not exist or will be detected [24, 18].

4 Conclusions

This paper has pointed out security flaws in Zou et al.'s AQS schemes, in which Trent cannot arbitrate a dispute between Alice and Bob when Bob claims a failure in the signature verification phase. Besides, a malicious verifier, Bob, can actively negate a signed order from Alice without being detected to get some benefits in his favor. In addition, we demonstrate that a malicious signatory can reveal the verifier's secret key by launching Trojan-horse attacks on Zou et al.'s AQS scheme. How to design an AQS scheme without the DoS attack and how to construct an AQS scheme free from Trojan-horse attacks without using any hardware device will be an interesting future research.

Acknowledgment

The authors would like to thank the anonymous reviewers for their very valuable comments that enhance the clarity of this paper a lot. We also like to thank the National Science Council of Republic of China and the Research Center of Quantum Communication and Security, National Cheng Kung University, Taiwan, R.O.C. for financial support of this research under Contract No. NSC 100-2221-E-006-152-MY3 and D100-36002, respectively.

References

- [1] G. H. Zeng and C. H. Keitel, “Arbitrated quantum-signature scheme,” *Physical Review A*, vol. 65, no. 4, p. 042312, 2002.
- [2] T. Hwang, S. K. Chong, Y. P. Luo, and T. X. Wei, “New arbitrated quantum signature of classical messages against collective amplitude damping noise,” *Optics Communications*, vol. 284, no. 12, pp. 3144–3148, Jun. Jan. 2011.
- [3] D. Gottesman and I. Chuang, “Quantum digital signatures,” arXiv:quant-ph/0105032v2, 15 Nov. 2001.
- [4] Y. G. Yang and Q. Y. Wen, “Arbitrated quantum signature of classical messages against collective amplitude damping noise,” *Optics Communications*, vol. 283, no. 16, pp. 3198–3201, Aug. 2010.
- [5] S. K. Chong, Y. P. Luo, and T. Hwang, “On “arbitrated quantum signature of classical messages against collective amplitude damping noise”,” *Optics Communications*, vol. 284, no. 3, pp. 893–895, Feb. 2011.
- [6] M. Curty and N. Lütkenhaus, “Comment on “arbitrated quantum-signature scheme”,” *Physical Review A*, vol. 77, no. 4, p. 046301, 2008.

- [7] G. H. Zeng, “Reply to ‘comment on ‘arbitrated quantum-signature scheme’”,” *Physical Review A*, vol. 78, no. 1, p. 016301, 2008.
- [8] Q. Li, W. H. Chan, and D.-Y. Long, “Arbitrated quantum signature scheme using Bell states,” *Physical Review A*, vol. 79, no. 4, p. 054307, 2009.
- [9] Y. G. Yang and Q. Y. Wen, “Erratum: Arbitrated quantum signature of classical messages against collective amplitude damping noise,” *Optics Communications*, vol. 283, no. 19, p. 3830, Oct. 2010.
- [10] J. Wang, Q. Zhang, L. M. Liang, and C. J. Tang, “Comment on: ‘arbitrated quantum signature scheme with message recovery’”,” *Physics Letters A*, vol. 347, pp. 262–263, 2005.
- [11] H. Lee, C. Hong, H. Kim, J. Lim, and H. J. Yang, “Arbitrated quantum signature scheme with message recovery,” *Physics Letters A*, vol. 321, pp. 295–300, 2004.
- [12] J. Wang, Q. Zhang, and C. J. Tang, “Quantum signature scheme with single photons,” *Optoelectronics Letters*, vol. 2, no. 2, pp. 209–212, May 2006.
- [13] X. J. Wen and Y. Liu, “Authentic digital signature based on quantum correlation,” arXiv:quant-ph/0509129v2, 11 Dec. 2006.
- [14] X. J. Wen and Y. Liu, “Quantum message signature scheme without an arbitrator,” in *The First International Symposium on Data, Privacy, and E-Commerce (ISDPE 2007)*, Chengdu, China, 01-03 Nov. 2007, pp. 496–500.
- [15] X. Zou and D. Qiu, “Security analysis and improvements of arbitrated quantum signature schemes,” *Physical Review A*, vol. 82, no. 4, p. 042325, 2010.

- [16] Q. Y. Cai, “The ping-pong protocol can be attacked without eavesdropping,” *Physical Review Letters*, vol. 91, no. 10, p. 109801, 2003.
- [17] —, “Eavesdropping on the two-way quantum communication protocols with invisible photons,” *Physics Letters A*, vol. 351, pp. 23–25, 2006.
- [18] F. G. Deng, P. Zhou, X. H. Li, C. Y. Li, and H. Y. Zhou, “Robustness of two-way quantum communication protocols against Trojan horse attack,” e-print quant-ph/0508168, 2005.
- [19] P. O. Boykin and V. Roychowdhury, “Optimal encryption of quantum bits,” *Physical Review A*, vol. 67, no. 4, p. 042317, 2003.
- [20] M. Curty, D. J. Santos, and E. Perez, “Qubit authentication,” *Physical Review A*, vol. 66, no. 2, p. 022301, 2002.
- [21] H. Barnum, C. Crepeau, and D. Gottesman, “Authentication of quantum messages,” in *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science*, Vancouver, BC, Canada, 16-19, Nov. 2002, p. 449.
- [22] P. G. Kwiat, K. Mattle, H. Weinfurter, and A. Zeilinger, “New high-intensity source of polarization-entangled photon pairs,” *Physical Review Letter*, vol. 75, no. 24, pp. 4337–4341, Dec. 1995.
- [23] H. Buhrman, R. Cleve, J. Watrous, and R. Wolf, “Quantum fingerprinting,” *Physical Review Letter*, vol. 87, no. 16, p. 167902, Oct. 2001.
- [24] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” *Reviews of Modern Physics*, vol. 74, pp. 145–195, 2002.